日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月１６日

出願番号
Application Number: 特願２００３－１１２１１０

[ST. 10/C]: ［ＪＰ２００３－１１２１１０］

出願人
Applicant(s): 日本電気株式会社

２００４年　１月２６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００２６３０

【書類名】　特許願
【整理番号】　53211064
【提出日】　平成15年 4月16日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/14
H04B 7/26
H04M 1/675
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　塚本　直史
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【代理人】
【識別番号】　100084250
【弁理士】
【氏名又は名称】　丸山　隆夫
【電話番号】　03-3590-8902
【手数料の表示】
【予納台帳番号】　007250
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9303564
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ユーザデータ保護方法、プログラムおよび携帯端末

【特許請求の範囲】

【請求項１】　ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、前記ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、

前記ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、

前記ユーザデータを前記識別情報毎に前記フォルダに分類するフォルダ分類ステップと、

前記識別情報を暗号鍵として用いて、前記ユーザデータを暗号化して保存する暗号化ステップと、

複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、

前記携帯端末内の前記ユーザデータを、前記ＵＩＭカード内の識別情報と関連付けし、前記ユーザデータを保護することを特徴とするユーザデータ保護方法。

【請求項２】　前記フォルダの作成は、前記携帯端末のユーザデータ保存領域に記録されることを特徴とする請求項１記載のユーザデータ保護方法。

【請求項３】　前記フォルダは、前記ＵＩＭカードの前記識別情報の数に応じて作成されることを特徴とする請求項１記載のユーザデータ保護方法。

【請求項４】　前記動的管理は、前記ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とする請求項１記載のユーザデータ保護方法。

【請求項５】　前記静的管理は、不揮発性メモリ上に固定領域を確保し、前記ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とする請求項１記載のユーザデータ保護方法。

【請求項６】　前記識別情報は、前記携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とする請求項１記載のユーザデータ保護方法。

【請求項７】　前記暗号処理ソフトウェアブロックは、前記ＵＩＭカードの挿入の有無に関わらず、前記携帯端末の電源オン時に起動されることを特徴とする請求項６記載のユーザデータ保護方法。

【請求項８】　前記暗号処理ソフトウェアブロックは、前記ユーザの操作によって、前記コンテンツが変更された場合、変更内容を暗号化した後で前記識別情報を暗号鍵として前記フォルダ内に保存することを特徴とする請求項６記載のユーザデータ保護方法。

【請求項９】　前記暗号処理ソフトウェアブロックは、前記ＵＩＭカードから読み出された前記識別情報を一時記憶することを特徴とする請求項７または８のいずれか１項に記載のユーザデータ保護方法。

【請求項１０】　前記暗号処理ソフトウェアブロックは、前記一時記憶した個人識別情報を用いて、前記携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とする請求項９記載のユーザデータ保護方法。

【請求項１１】　前記識別情報は、ＩＭＳＩおよびＩＣＣシリアルのいずれか一方であることを特徴とする請求項１から１０のいずれか１項に記載のユーザデータ保護方法。

【請求項１２】　前記フォルダは前記ユーザ操作によって作成されることを特徴とする請求項１記載のユーザデータ保護方法。

【請求項１３】　ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、

前記ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、

前記ユーザデータを前記識別情報毎に前記フォルダに分類するフォルダ分類処理と、

前記識別情報を暗号鍵として用いて、前記ユーザデータを暗号化して保存する暗号化処理と、

複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理と、

をコンピュータに実行させることを特徴とするプログラム。

【請求項１４】　請求項１から１２のいずれか１項に記載のユーザデータ保護方法を実施することを特徴とする携帯端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ＵＩＭカード等を用いて加入者情報と端末本体を分離保有可能な携帯端末に用いられるユーザデータ保護方法、プログラムおよび携帯端末に関する。

【０００２】

【従来の技術】

第三世代携帯電話機においては、加入者情報と携帯電話機本体が分離しており、ユーザは自身の加入者情報が記録されたＵＩＭカードを保有し、任意の携帯電話機に挿入してサービスを利用することが可能である。個人のプライバシーはＵＩＭカードに由来しており、契約情報も含めた重要な個人データは全てＵＩＭカード内に保持されることが理想である。

【０００３】

しかしながら、ＵＩＭカードのサイズ／容量上の制限により、ＵＩＭカードに全てユーザデータを保持することは不可能であり、メールや電話帳、アプリケーションなど、ユーザ個人が利用するコンテンツの殆どは携帯電話機本体に記録されることになる。

【０００４】

従って、ある個人の携帯電話機に他人のＵＩＭカードが挿入された場合、そのＵＩＭカードの契約情報に基づいたサービスを利用できると同時に、内部のコンテンツは他人によって自由に使用並びに変更ができることになる。例としては、①発着信履歴が残る。②挿入された他人のＵＩＭカードに宛てられたメール等が記録される。③ＮＷ利用型コンテンツの使用が可能となる（ＮＷ接続を利用するアプリケーション等）。④内蔵コンテンツの追加および削除、といった操作が可能となる。

【０００５】

また、ＵＩＭカードを挿入せずに携帯電話機の電源を投入した場合、携帯電話のサービスを利用することは不可能であるが、内部のコンテンツは自由に使用できる。

【０００６】

以上のことから、従来の日本国内における携帯電話機（第三世代以前）では、携帯電話機自体の不揮発領域に個人契約情報が記録されているため、「個人情報の管理＝携帯電話機内のコンテンツの管理」という図式が成立するが、第三世代においては前述の通り、契約情報を含めた個人データはＵＩＭカードに由来するため、１台の携帯電話機を複数の契約者で共有する機会が格段に増すことから、第３世代携帯における個人データを保護が必要となる。

【０００７】

従来の技術例として、ユーザデータを不揮発性メモリへ格納する構成の携帯端末において、ユーザデータの書き込み時の消失や不正化を防止する「携帯端末とそのユーザデータ保護方法」がある（例えば、特許文献１参照）。また、ユーザの識別情報やユーザが独自に決めた識別情報を、キーワードを用いて自動的に暗号化および解読する「情報の暗号化／解読方法と同システム」がある（例えば、特許文献２参照）。また、ＳＩＭカードを用いて利用した携帯電話機を他者に渡した場合、内部に記録されたプライベートな個人データの閲覧を防止できる「加入者カードを用いる携帯電話機」がある（例えば、特許文献３参照）。

【０００８】

【特許文献１】

特開２００１－１０１０７９号公報

【特許文献２】

特開２００２－２８１０２２号公報

【特許文献３】

特開２００２－３００２５４号公報

【０００９】

【発明が解決しようとする課題】

上記特許文献１記載の発明は、ＵＩＭカード等を使用する第３世代携帯端末に対応していない構成である。また、特許文献２記載の発明は、データの暗号化に用いるキーワードがユーザによって作成されるものであり、ＵＩＭカード内の識別情報を用いるものではなく、第３世代携帯端末に対応していない構成である。また、特許文献３記載の発明は、第３世代携帯に対応する構成ではあるが、データ保護のために外付けのメモリを必要とする。

【００１０】

よって、外付けの装置を必要とせず、第３世代携帯端末の構成に対応可能であり、ＵＩＭカードなしで端末の電源を入れた際に、内部のユーザデータの閲覧を不可能とするユーザデータ保護方法が望まれる。

【００１１】

本発明は、上記事情に鑑みてなされたものであり、ＵＩＭカード等により加入者情報と本体を分離保有可能な携帯端末において、携帯端末内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護するユーザデータ保護方法、プログラムおよび携帯端末を提供することを目的とする。

【００１２】

また、本発明は、携帯電話機が複数の契約者によって共有利用されることを前提とし、本体に記録されるコンテンツのプライバシー保護について、ＵＩＭカード内の識別情報（ＩＭＳＩ）を関連させ、他人のＵＩＭカードが挿入された場合にも、暗号鍵となるＵＩＭカードの識別情報が異なるため、他人内部のユーザデータの閲覧が不可能となるユーザデータ保護方法、プログラムおよび携帯端末を提供することを目的とする。

【００１３】

【課題を解決するための手段】

かかる目的を達成するために、請求項１記載のユーザデータ保護方法は、ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類する

フォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータを、ＵＩＭカード内の識別情報と関連付けし、ユーザデータを保護することを特徴とする。

【００１４】

請求項２記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、フォルダの作成は、携帯端末のユーザデータ保存領域に記録されることを特徴とする。

【００１５】

請求項３記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、フォルダは、ＵＩＭカードの前記識別情報の数に応じて作成されることを特徴とする。

【００１６】

請求項４記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、動的管理は、ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とする。

【００１７】

請求項５記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、静的管理は、不揮発性メモリ上に固定領域を確保し、ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とする。

【００１８】

請求項６記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、識別情報は、携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とする。

【００１９】

請求項７記載のユーザデータ保護方法は、請求項６記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ＵＩＭカードの挿入の有無に関わらず、携帯端末の電源オン時に起動されることを特徴とする。

【００２０】

請求項８記載のユーザデータ保護方法は、請求項６記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ユーザの操作によって、コンテンツが変更された場合、変更内容を暗号化した後で識別情報を暗号鍵としてフォルダ内に保存することを特徴とする。

【００２１】

請求項９記載のユーザデータ保護方法は、請求項７または８のいずれか１項に記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ＵＩＭカードから読み出された識別情報を一時記憶することを特徴とする。

【００２２】

請求項１０記載のユーザデータ保護方法は、請求項９記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、一時記憶した個人識別情報を用いて、携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とする。

【００２３】

請求項１１記載のユーザデータ保護方法は、請求項１から１０のいずれか１項に記載のユーザデータ保護方法において、識別情報は、ＩＭＳＩおよびＩＣＣシリアルのいずれか一方であることを特徴とする。

【００２４】

請求項１２記載のユーザデータ保護方法は、請求項１記載のユーザデータ保護方法において、フォルダはユーザ操作によって作成されることを特徴とする。

【００２５】

請求項１３記載のプログラムは、ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類処理と、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化処理と、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理とをコンピュータに

実行させることを特徴とする。

【００２６】

請求項１４記載の携帯端末は、請求項１から１２のいずれか１項に記載のユーザデータ保護方法を実施することを特徴とする。

【００２７】

【発明の実施の形態】

以下、本発明の実施形態について、添付図面を参照しながら詳細に説明する。

【００２８】

ＵＩＭカード等により加入者情報と本体を分離保有可能な携帯電話機の一般的な装置構成を図２に示す。ＵＩＭカード８にはＩＭＳＩ（International Mobile Station Identifer）と呼ばれる、加入者情報を識別するための唯一無二の情報要素が内包されている。利用者はこのＵＩＭカード８を携帯電話機本体に装着することにより、携帯電話網への接続し、契約するサービスを利用することができる。携帯電話機本体はユーザデータを永続的に保存するための不揮発性メモリ１１（あるいは常時バックアップされる揮発性メモリ）を有している。

【００２９】

ユーザデータとは電話帳、メール、発着信履歴、その他のコンテンツ、更には携帯電話機操作部のカスタマイズ情報（例えば、画面上に置かれたアイコンの配置情報）なども指し示す。

【００３０】

図３に示すように、ユーザデータの保存方法としては、1つ1つのコンテンツを各々固定サイズのエリアに格納する方式（静的管理方式）や、可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理する方式（動的管理方式）などがある。これらのユーザデータは、装置電源ＯＮ時、あるいはユーザ操作によりデータ読出し時に、不揮発性メモリ領域から一旦一時メモリ領域に展開されて利用される。ユーザデータの変更等は、まず一時メモリ領域に展開されたデータを変更し、不揮発メモリ領域に反映される。不揮発メモリ領域を書き換えるタイミングは、コンテンツ毎の性質により異なる。

【００３１】

次に本発明における、ユーザデータの保護方法のイメージを図１に示す。本発明において、携帯電話機内のユーザデータは動的管理されることを前提とする。携帯電話機のユーザデータ保存領域には、ＩＭＳＩに関連付けられた「フォルダ」情報が記録され、個人のユーザデータは契約しているＵＩＭカードのＩＭＳＩに従って、フォルダ分けされる。このフォルダ情報は携帯電話機を共有使用するＵＩＭカードのＩＭＳＩの数だけ作成される。必要に応じてユーザ操作により、新たなフォルダを作成することも可能とする。また、共通に利用できるコンテンツを保存する機能を有するため、「共有フォルダ」が作成される。

【００３２】

さらに、携帯電話機は、図２の中央制御部内にＵＩＭ内のＩＭＳＩを用いた暗号化／解読処理を実施する暗号処理ソフトウェアブロック１３を有している。この暗号処理ソフトウェアブロック１３の機能は大きく以下の通りである。

（１）ＵＩＭカードより読み出されたＩＭＳＩ情報を一時記憶する機能（他のソフトウェアブロックと共通でありうる）。

（２）一時記憶されたＩＭＳＩを用いて、携帯電話機内のコンテンツを暗号化／暗号解読処理を実施する機能。

【００３３】

携帯電話機のメインプログラムは、装置電源ＯＮ時にＵＩＭカードが挿入有無に関わらず、必ずこの暗号処理ブロックを起動する。また、携帯電話機操作にて内蔵するコンテンツ情報が変更された場合は、必ずこの暗号処理ソフトウェアブロック１３を起動し、ＩＭＳＩを暗号鍵として変更内容を暗号化した後で、ＩＭＳＩに関連されたフォルダ内に保存する。

【００３４】

例えば、図４において、ＩＭＳＩ＝［Ｂ］というＵＩＭカードが使用されている場合は、ＩＭＳＩに関連付けられたフォルダ内のファイルと、共有フォルダ内のファイルのみが移動機本体にて使用可能となる。

【００３５】

次に、図５から図７を参照して本発明の実施形態の動作を説明する。

【００３６】

装置電源投入時の動作について図５を参照して説明する。中央制御部に電源供給開始し、装置の初期設定を行う（Ｓ５０１）。ＵＩＭカードが装置に挿入されているかを調べる（Ｓ５０２）。挿入されていない場合は（Ｓ５０２／ＮＯ）、暗号処理ブロックを起動する（Ｓ５０６）。挿入されている場合（Ｓ５０２／ＹＥＳ）、本体に挿入されたＵＩＭカードを活性化し（Ｓ５０３）、さまざまな情報を読み出す（Ｓ５０４）。ＵＩＭカードより読み出したＩＭＳＩを一時記憶する（Ｓ５０５）。暗号処理ブロックを起動する（Ｓ５０６）。メインプログラムが「共有フォルダ」内の情報を読出す（Ｓ５０７）。このフォルダ内の情報は暗号解読を行わない。メインプログラムが一時記憶されたＩＭＳＩが存在し（Ｓ５０８／ＹＥＳ）、ＩＭＳＩに関連付けられたフォルダ（ＩＭＳＩ固有フォルダ）がある場合（Ｓ５０９／ＹＥＳ）、一時記憶ＩＭＳＩを参照し、ＩＭＳＩ固有フォルダ内の情報を読み出す（Ｓ５１０）。暗号処理ブロックが一時記憶されたＩＭＳＩを暗号鍵として、ユーザデータ保存領域のデータを読出し、解読する（Ｓ５１１）。共有データと解読されたユーザデータを、一時メモリ領域に展開する（Ｓ５１２）。一時記憶ＩＭＳＩ、ＩＭＳＩ固有フォルダのどちらかがない場合は（Ｓ５０８／ＮＯ、Ｓ５０９／ＮＯ）、読み出しおよび処理を行わず、そのまま共有データと解読されたユーザデータを、一時メモリ領域に展開する（Ｓ５１２）。

【００３７】

装置操作によるユーザデータ読出し時の動作について図６を参照して説明する。指定したユーザデータが共有データの場合（Ｓ６０１／ＹＥＳ）、「共有フォルダ」より情報を読出し（Ｓ６０３）、暗号解読せずに指定データを展開する（Ｓ６０９）。指定したユーザデータがＩＭＳＩに関連付けられた暗号化データの場合（Ｓ６０２／ＮＯ、Ｓ６０４／ＹＥＳ、Ｓ６０５／ＹＥＳ）、暗号化ブロックを起動する（Ｓ６０６）。ＩＭＳＩに関連づけられたフォルダより情報を読出す（Ｓ６０７）。記憶したＩＭＳＩを用いて暗号を解読する（Ｓ６０８）。指定データを展開する（Ｓ６０９）。

【００３８】

装置操作によるユーザデータ保存時の動作について図７を参照して説明する。

電話帳入力やメール送受信、ＮＷからのダウンロード等によって得られたコンテンツが一時的メモリ領域に記録される。得られたコンテンツの保存操作を実行する。このとき、共有データとして保存するか、暗号化して保存するかの選択をユーザ操作により指定できることとする（Ｓ７０１）。指定したユーザデータが共有データの場合（Ｓ７０２／ＹＥＳ）、「共有フォルダ」内に暗号化無しで保存する（Ｓ７０３）。

【００３９】

指定したユーザデータがＩＭＳＩに関連付けられた暗号化データの場合（Ｓ７０２／ＮＯ、Ｓ７０４／ＹＥＳ、Ｓ７０５／ＹＥＳ）、暗号化ブロックを起動する（Ｓ７０６）。暗号解読処理後（Ｓ７０７）、一時メモリ領域上のユーザデータに対して、ＩＭＳＩを暗号鍵とした暗号化処理を実施し（Ｓ７０８）、指定の不揮発保存領域に記憶する。Ｓ７０５においてＩＭＳＩ固有フォルダがない場合（Ｓ７０５／ＮＯ）、ＩＭＳＩ固有フォルダを作成するかを選択し（Ｓ７０９）、フォルダ作成後（Ｓ７１０）、暗号処理ブロックを起動し（Ｓ７０６）、同様の処理を行う。

【００４０】

以上、本発明の実施形態によれば、第１の効果として、ＵＩＭカードにより加入者情報と本体を分離保有可能な携帯電話機において、携帯電話機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。第２の効果として、上記識別情報に関連した個人の固有データを、同じく識別情報に基づいて暗号化することにより、個人の固有データ保護を強固にできる。

【００４１】

また、他の実施形態１として、暗号化処理とフォルダ分けをＩＭＳＩではなく、同じくＵＩＭカードの固有情報である「ＩＣＣシリアル」によって行うことも可能である。また、他の実施形態２として、静的管理において、本発明の概念を適用した場合、不揮発性メモリ上に固定領域を確保する。複数ユーザでシェアする場合、ユーザごとに固定エリアを割当てることは無駄が多いため、固有のユーザデータのヘッダ部分にタグをつけて、どのユーザによって利用可能かを判断する手段がある。

【００４２】

【発明の効果】

以上の説明から明らかなように、請求項１記載のユーザデータ保護方法によれば、ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末で用いられ、ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータを、ＵＩＭカード内の識別情報と関連付けし、ユーザデータを保護することを特徴とするので、ＵＩＭカードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人のＵＩＭカードが挿入された場合でも、暗号鍵となるＵＩＭカードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【００４３】

請求項２記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、フォルダの作成は、携帯端末のユーザデータ保存領域に記録されることを特徴とするので、携帯電話機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。

【００４４】

請求項３記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、フォルダは、ＵＩＭカードの前記識別情報の数に応じて作成されることを特徴とするので、携帯電話機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。

【００４５】

請求項４記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、動的管理は、ユーザデータを可変サイズのファイルとして記憶し、ファイル管理テーブルを用いて管理することを特徴とするので、携帯電話

機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。

【００４６】

請求項５記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、静的管理は、不揮発性メモリ上に固定領域を確保し、ユーザデータのヘッダ部分にタグをつけて、利用可能なユーザを判断することを特徴とするので、携帯電話機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。

【００４７】

請求項６記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、識別情報は、携帯端末が有する暗号処理ソフトウェアブロックによって暗号化処理され、暗号鍵となることを特徴とするので、個人の固有データ保護を強固にする。

【００４８】

請求項７記載のユーザデータ保護方法によれば、請求項６記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ＵＩＭカードの挿入の有無に関わらず、携帯端末の電源オン時に起動されることを特徴とするので、個人の固有データ保護を強固にする。

【００４９】

請求項８記載のユーザデータ保護方法によれば、請求項６記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ユーザの操作によって、コンテンツが変更された場合、変更内容を暗号化した後で識別情報を暗号鍵としてフォルダ内に保存することを特徴とするので、個人の固有データ保護を強固にする。

【００５０】

請求項９記載のユーザデータ保護方法によれば、請求項７または８のいずれか１項に記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、ＵＩＭカードから読み出された識別情報を一時記憶することを特徴とするので、個人の固有データ保護を強固にする。

【００５１】

請求項１０記載のユーザデータ保護方法によれば、請求項９記載のユーザデータ保護方法において、暗号処理ソフトウェアブロックは、一時記憶した個人識別情報を用いて、携帯端末内のコンテンツの暗号化および暗号解読処理を行うことを特徴とするので、個人の固有データ保護を強固にする。

【００５２】

請求項１１記載のユーザデータ保護方法によれば、請求項１から１０のいずれか１項に記載のユーザデータ保護方法において、識別情報は、ＩＭＳＩおよびＩＣＣシリアルのいずれか一方であることを特徴とするので、どちらの識別情報でも暗号化ができ、個人の固有データ保護を強固にする。

【００５３】

請求項１２記載のユーザデータ保護方法によれば、請求項１記載のユーザデータ保護方法において、フォルダはユーザ操作によって作成されることを特徴とするので、携帯電話機内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護できる。

【００５４】

請求項１３記載のプログラムによれば、ＵＩＭカードの使用によりユーザデータを本体から分離保有する携帯端末のユーザデータ保護方法をコンピュータに実行させるプログラムであって、ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成処理と、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類処理と、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化処理と、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成処理とをコンピュータに実行させることを特徴とするので、ＵＩＭカードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人のＵＩＭカードが挿入された場合でも、暗号鍵となるＵＩＭカードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【００５５】

請求項１４記載の携帯端末によれば、請求項１から１２のいずれか１項に記載

のユーザデータ保護方法を実施することを特徴とするので、ＵＩＭカードなしで携帯電話機の電源を投入した際、内部のユーザデータの閲覧を不可能とし、また、他人のＵＩＭカードが挿入された場合でも、暗号鍵となるＵＩＭカードの識別情報が異なるため、他人の内部ユーザデータ閲覧が不可能となる。

【図面の簡単な説明】

【図１】

本発明のユーザデータ保護方法を示すイメージ図である。

【図２】

本発明の実施形態である携帯電話の構成を示すブロック図である。

【図３】

従来のユーザデータ管理方法を示すイメージ図である。

【図４】

本発明のＵＩＭカードが挿入された場合の使用可能なデータの一例を示すイメージ図である。

【図５】

本発明の実施形態にかかる装置電源投入時の処理動作を示すフロー図である。

【図６】

本発明の実施形態にかかるユーザデータ読み出し時の処理動作を示すフロー図である。

【図７】

本発明の実施形態にかかるユーザデータ保存時の処理動作を示すフロー図である。

【符号の説明】

１　無線部

２　通信処理部

３　中央制御部

４　周辺制御部

５　電源制御部

６　共通バス

７　ＵＩＭカード制御部

８　ＵＩＭカード

９　レシーバ

１０　マイク

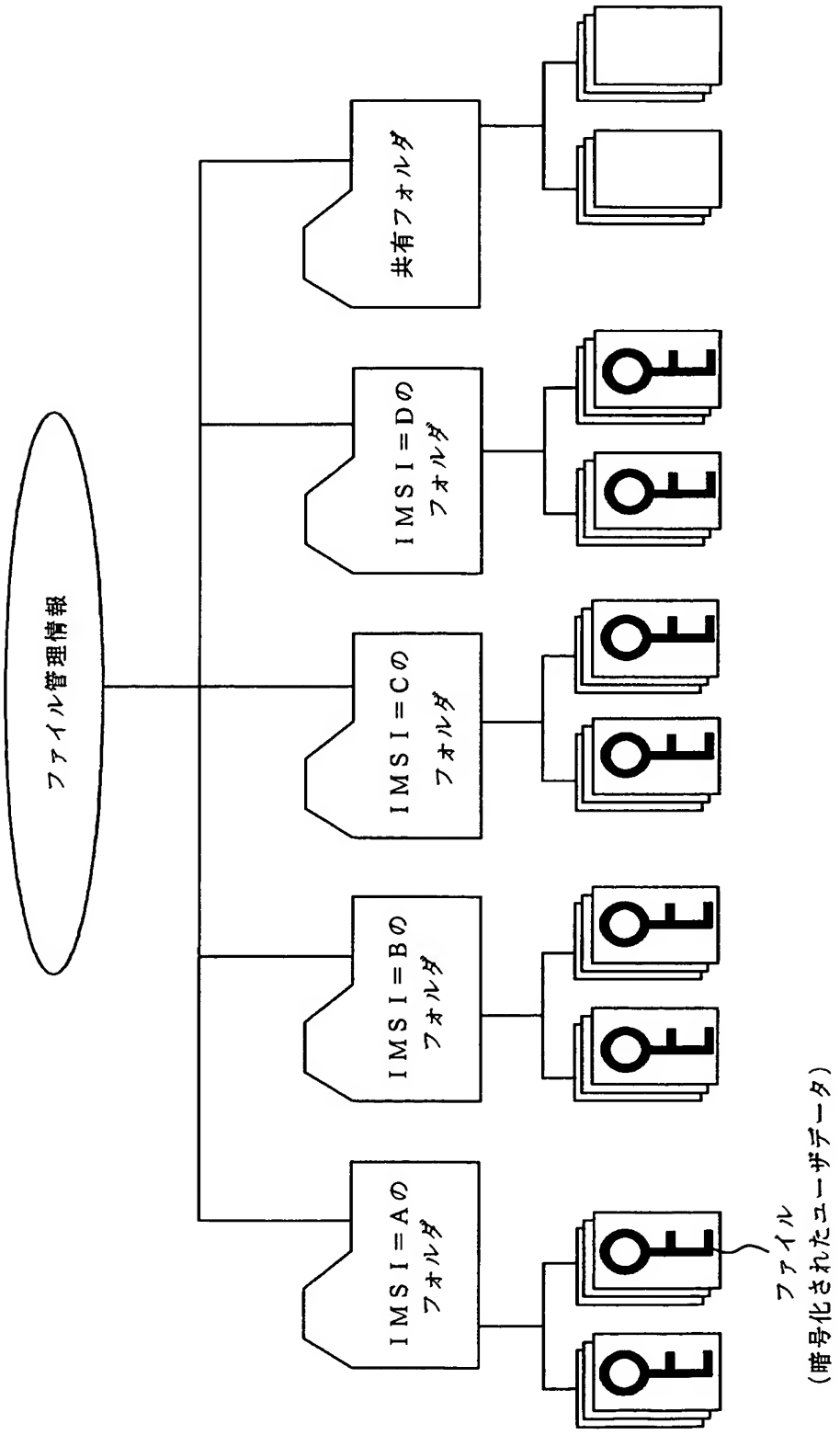
１１　不揮発メモリ

１２　一時記憶用メモリ

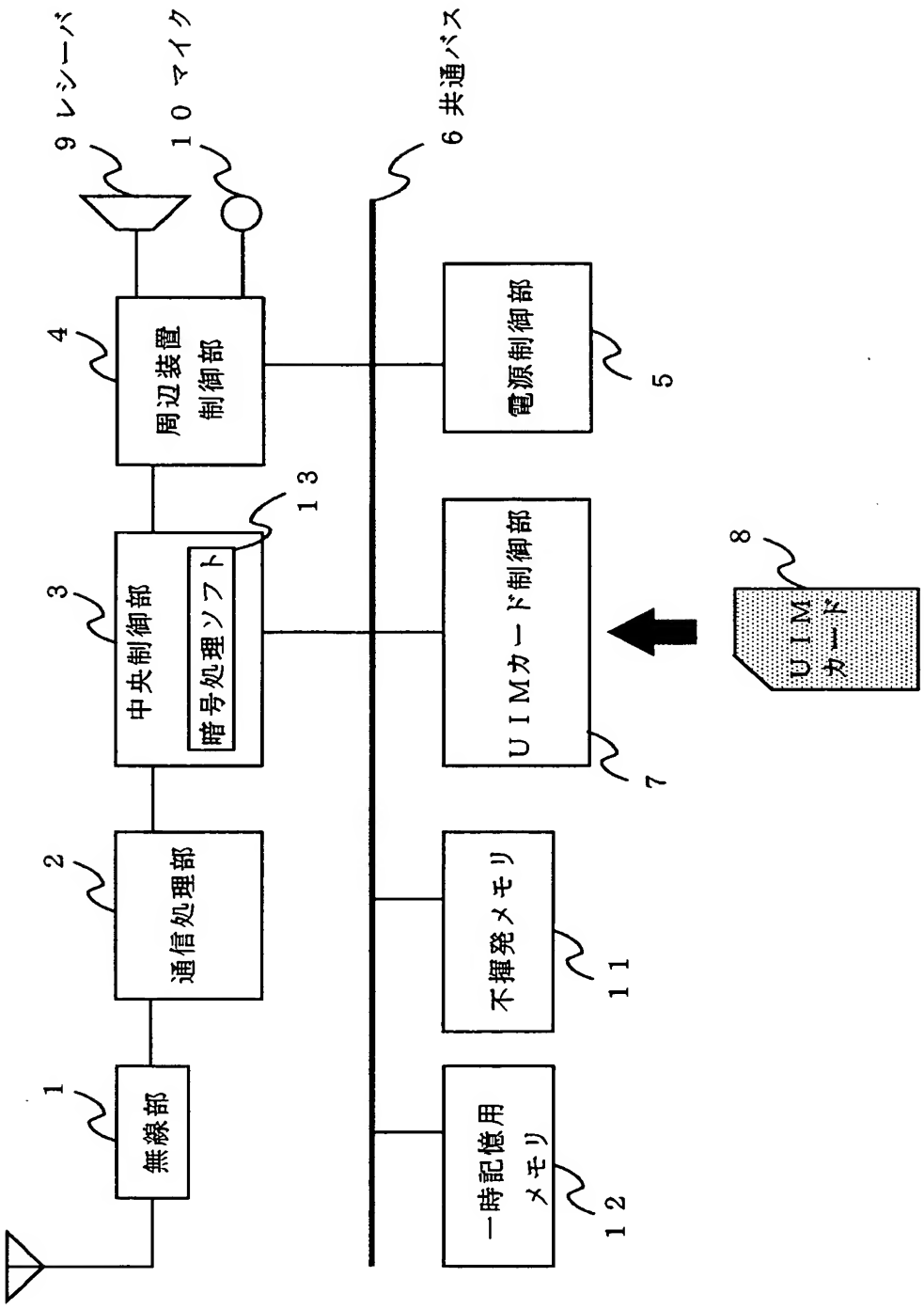
１３　暗号処理ソフト

【書類名】　　図面

【図１】

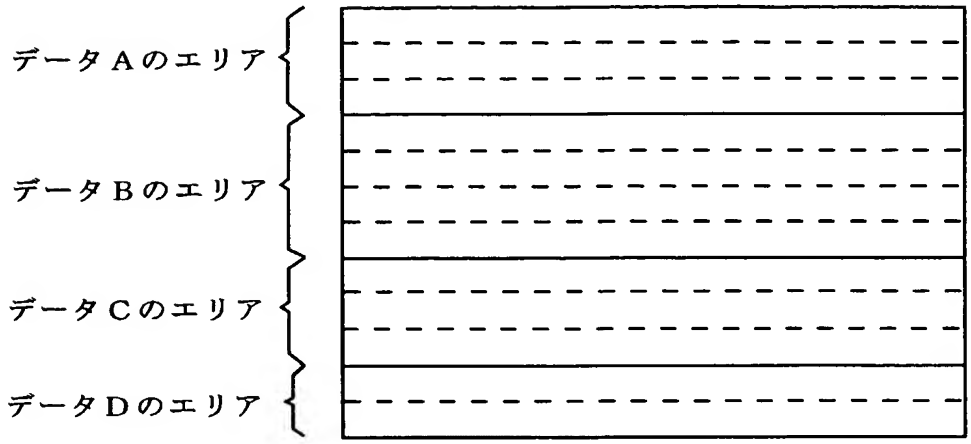

ファイル管理情報
共有フォルダ
ＩＭＳＩ＝Ｄの
フォルダ
ＩＭＳＩ＝Ｃの
フォルダ
ＩＭＳＩ＝Ｂの
フォルダ
ＩＭＳＩ＝Ａの
フォルダ
ファイル
（暗号化されたユーザデータ）

【図２】

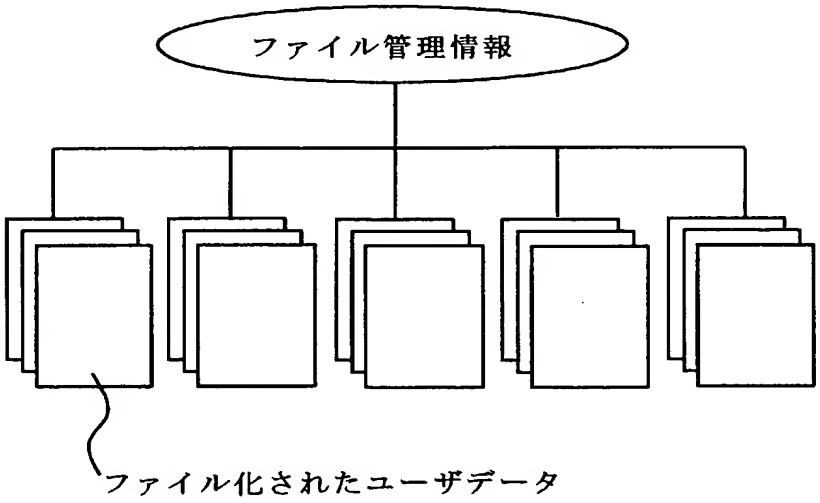

９レシーバ
１０マイク
６共通バス
４
周辺装置
制御部
５
電源制御部
１３
３
中央制御部
暗号処理ソフト
８
ＵＩＭ
カード
ＵＩＭカード制御部
７
２
通信処理部
不揮発メモリ
１１
１
無線部
一時記憶用
メモリ
１２

【図３】

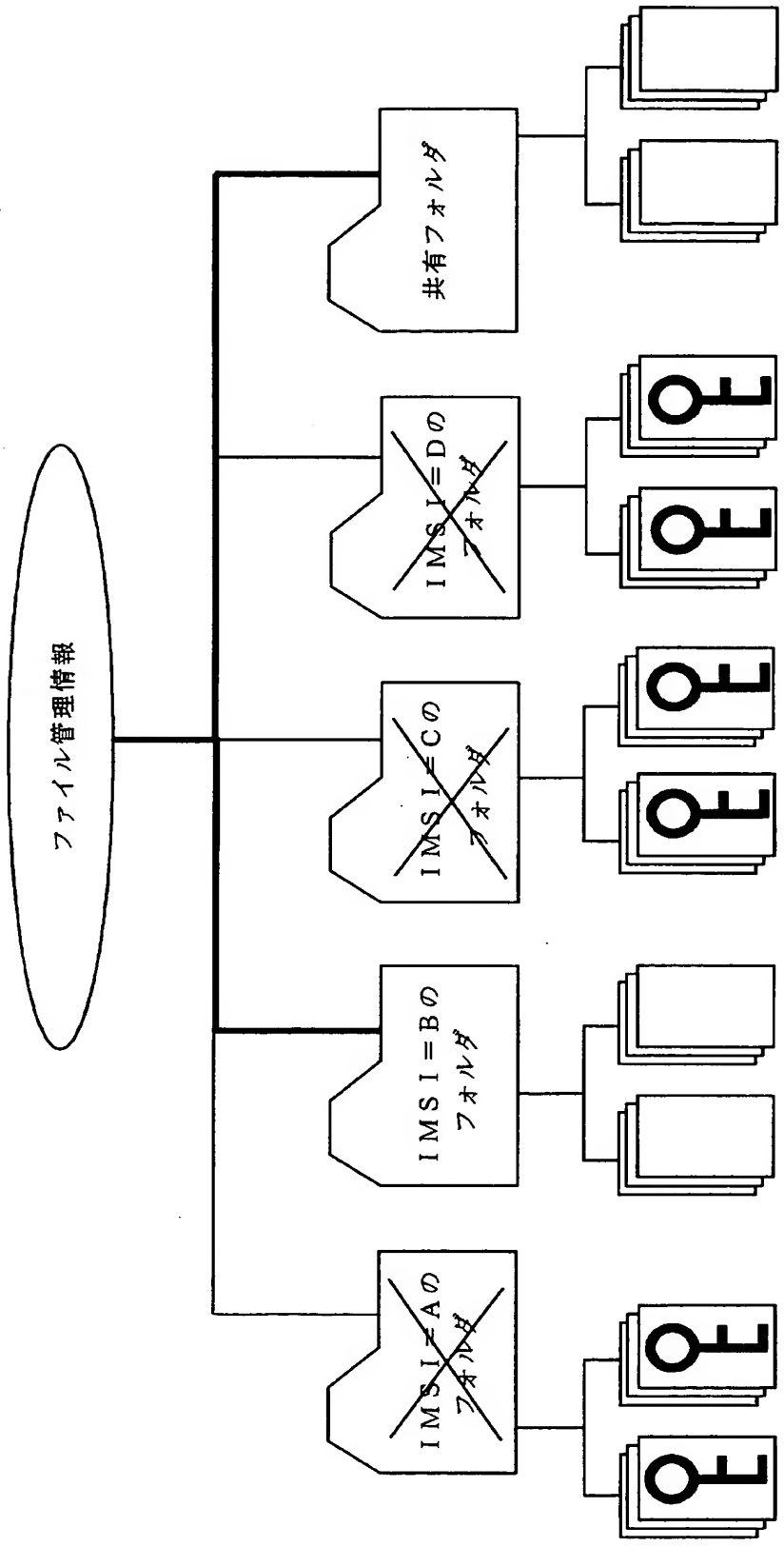
（ａ）ユーザデータを静的管理する場合



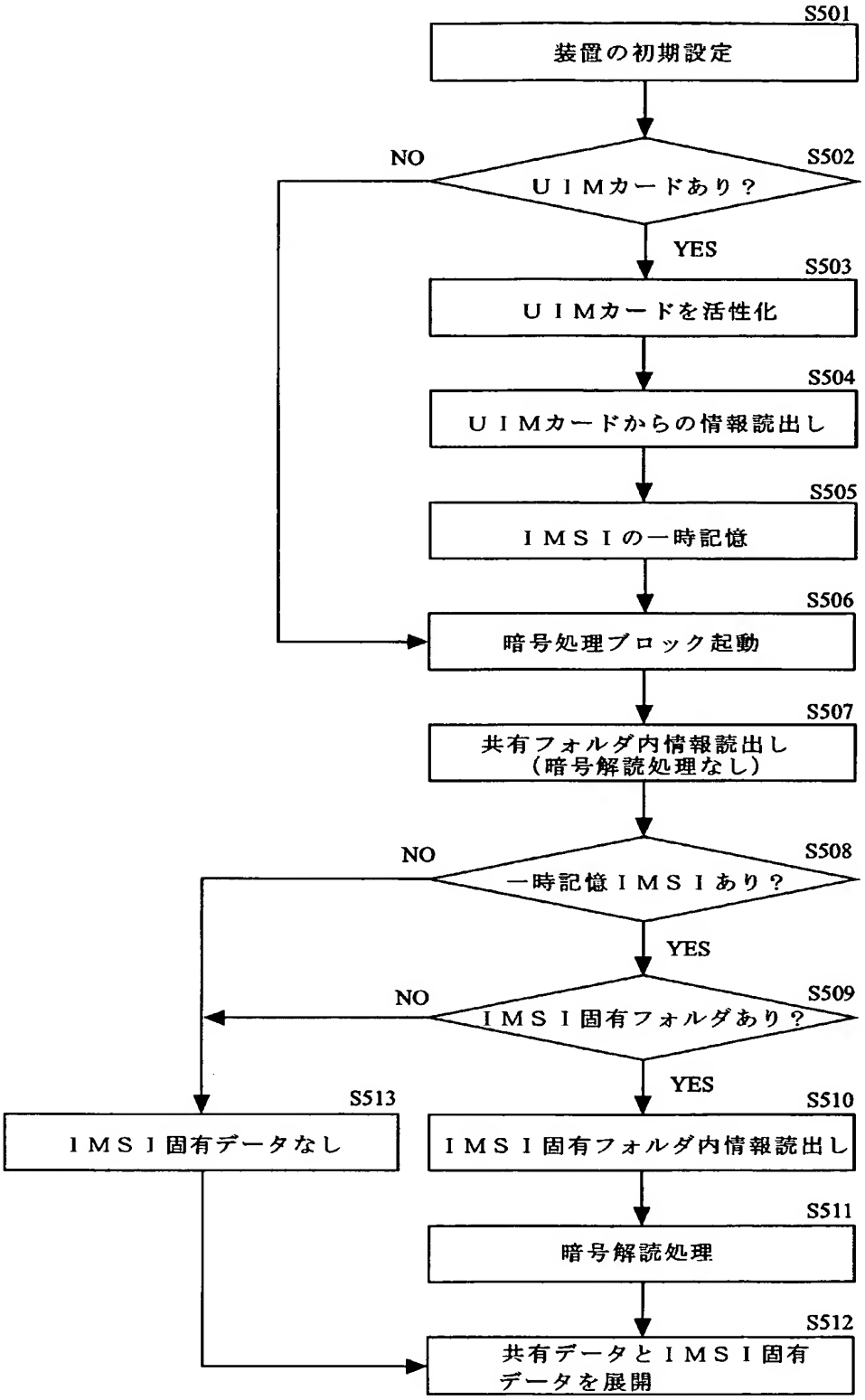
（ｂ）ユーザデータを静的管理する場合



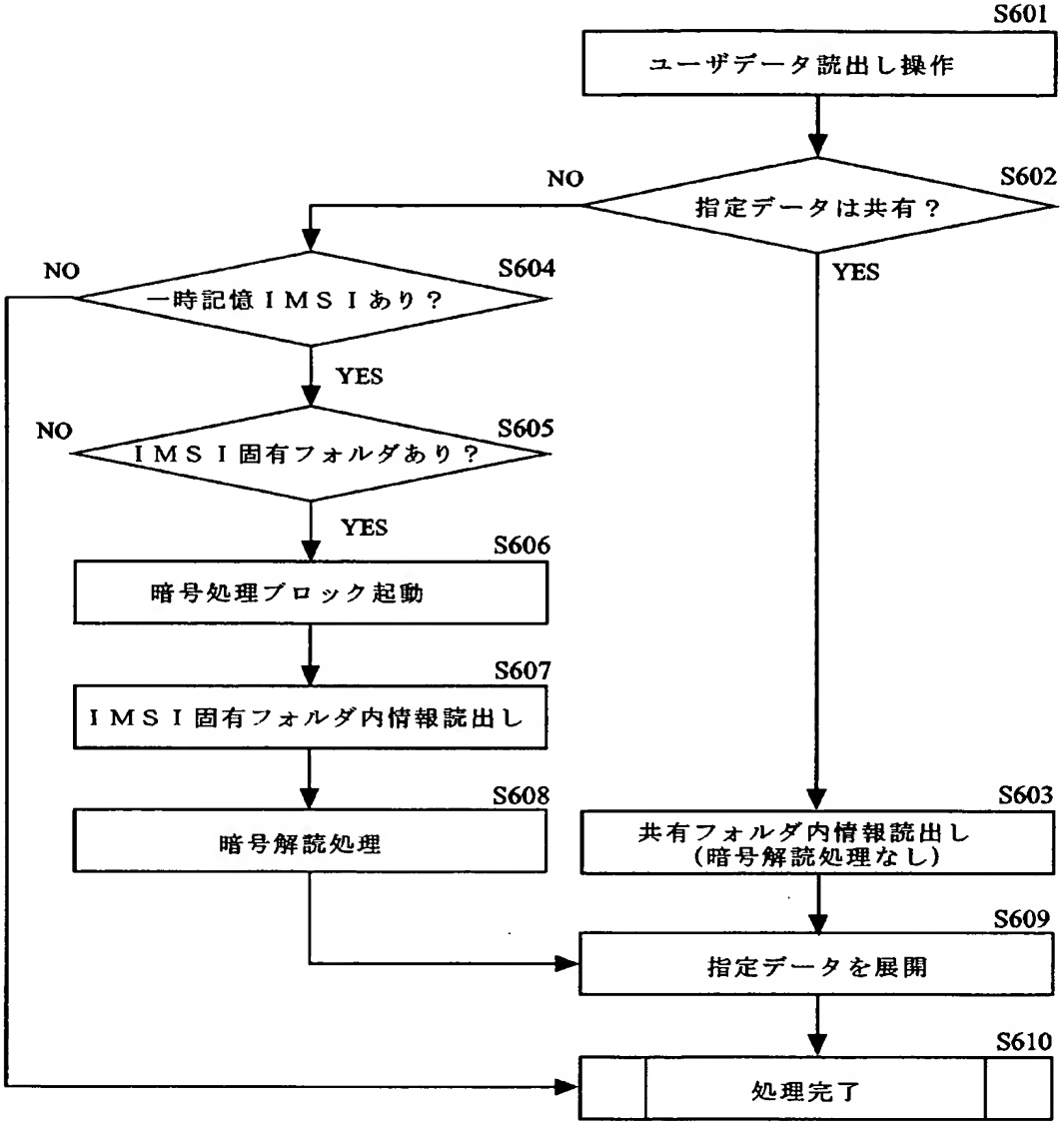
【図４】


ファイル管理情報
共有フォルダ
IMSI＝Dのフォルダ
IMSI＝Cのフォルダ
IMSI＝Bのフォルダ
IMSI＝Aのフォルダ

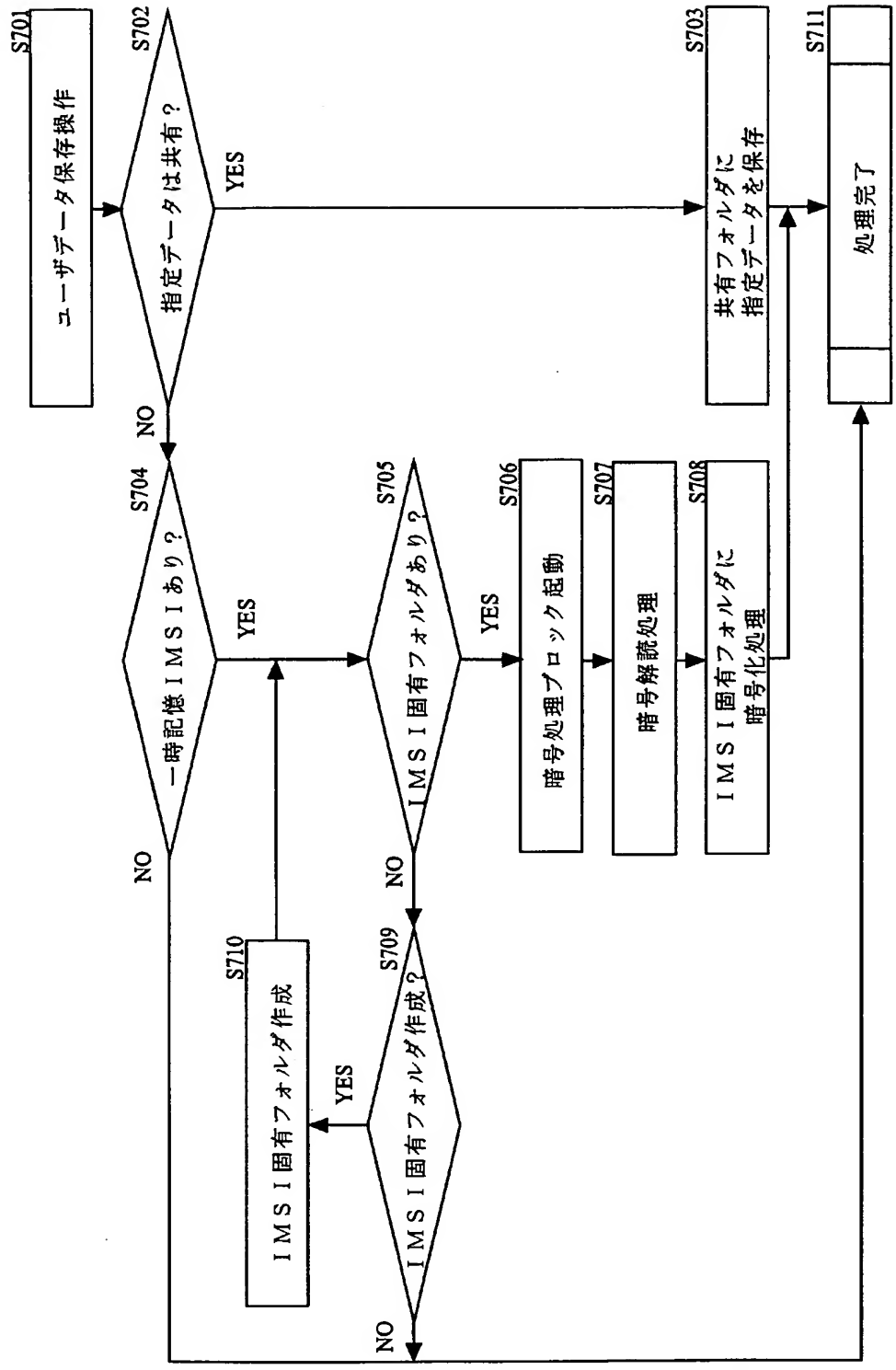
【図５】


S501
装置の初期設定
S502
ＵＩＭカードあり？
NO
YES
S503
ＵＩＭカードを活性化
S504
ＵＩＭカードからの情報読出し
S505
ＩＭＳＩの一時記憶
S506
暗号処理ブロック起動
S507
共有フォルダ内情報読出し
（暗号解読処理なし）
S508
一時記憶ＩＭＳＩあり？
NO
YES
S509
ＩＭＳＩ固有フォルダあり？
NO
YES
S513
ＩＭＳＩ固有データなし
S510
ＩＭＳＩ固有フォルダ内情報読出し
S511
暗号解読処理
S512
共有データとＩＭＳＩ固有
データを展開

【図６】


S601
ユーザデータ読出し操作
S602
指定データは共有？
NO
YES
S604
一時記憶ＩＭＳＩあり？
NO
YES
S605
ＩＭＳＩ固有フォルダあり？
NO
YES
S606
暗号処理ブロック起動
S607
ＩＭＳＩ固有フォルダ内情報読出し
S608
暗号解読処理
S603
共有フォルダ内情報読出し
（暗号解読処理なし）
S609
指定データを展開
S610
処理完了

【図７】


S701
ユーザデータ保存操作
S702
指定データは共有？
YES
NO
S703
共有フォルダに
指定データを保存
S704
一時記憶ＩＭＳＩあり？
YES
NO
S705
ＩＭＳＩ固有フォルダあり？
YES
NO
S706
暗号処理ブロック起動
S707
暗号解読処理
S708
ＩＭＳＩ固有フォルダに
暗号化処理
S709
ＩＭＳＩ固有フォルダ作成？
YES
NO
S710
ＩＭＳＩ固有フォルダ作成
S711
処理完了

【書類名】　要約書

【要約】

【課題】　携帯端末内のユーザデータをＵＩＭカード内の識別情報と関連付けし、個人の固有データを保護するユーザデータ保護方法、プログラムおよび携帯端末を提供する。

【解決手段】　ユーザデータを静的管理および動的管理のいずれか一方で管理するユーザデータ保護方法であって、ＵＩＭカードの識別情報に関連付けられたフォルダを作成するフォルダ作成ステップと、ユーザデータを識別情報毎にフォルダに分類するフォルダ分類ステップと、識別情報を暗号鍵として用いて、ユーザデータを暗号化して保存する暗号化ステップと、複数のユーザによって共通に利用されるコンテンツを保存するための共有フォルダを作成する共有フォルダ作成ステップとを有し、携帯端末内のユーザデータをＵＩＭカード内の識別情報と関連付けし、ユーザデータを保護する。

【選択図】　図１

特願２００３－１１２１１０

出　願　人　履　歴　情　報

識別番号　［０００００４２３７］

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社